Prevention of spoofing in telecommunications systems

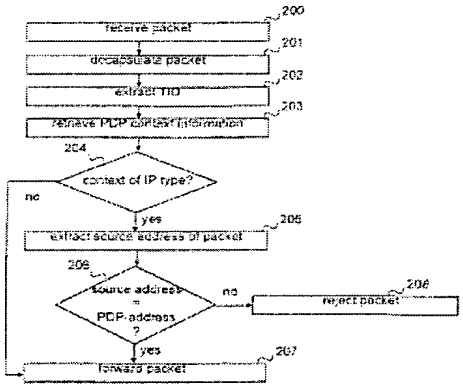
Patent number: JP2003518821T
Publication date: 2003-06-10
Inventor:
Applicant:
Classification:
- international: ***H04L12/56; H04L29/06; H04L29/08; H04L29/12;*** *H04Q7/22;* **H04L12/56; H04L29/06; H04L29/08; H04L29/12;** H04Q7/22; (IPC1-7): H04L12/56; H04Q7/38
- european: H04L29/06C6G; H04L12/56B; H04L29/06J1; H04L29/08A7W; H04L29/12A
Application number: JP20010547792T 20001219
Priority number(s): FI19990002767 19991222; WO2000FI01114 20001219

Also published as:
WO0147179 (A1)
US2002181448 (A1)
FI110975B (B)

Report a data error here

Abstract not available for JP2003518821T
Abstract of corresponding document: **US2002181448**

In a packet radio network a packet data address is activated for a terminal for transmitting data packets between the terminal and an external network. Information on the activated packet data address is stored at least in the edge nodes of the network. To prevent spoofing, i.e. misrepresentation of sender data, the method and network node of the invention comprise checking (206) in the node whether the source address of the packet transmitted from the terminal is the same as the packet data address used in the transmission of the packet or does the source address belong to a set of allowed packet data addresses. The packet is transmitted (207) from the node towards the destination address only if the addresses are identical or the source address belongs to the set of allowed packet data addresses.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁(JP)　(12)公表特許公報（A）　(11)特許出願公表番号

特表２００３－５１８８２１
（Ｐ２００３－５１８８２１Ａ）
(43)公表日　平成15年6月10日(2003.6.10)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ　12/56	１００	Ｈ０４Ｌ　12/56	１００　Ｚ	5K030
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９　Ｒ	5K067

審査請求　有　予備審査請求　有　（全２６頁）

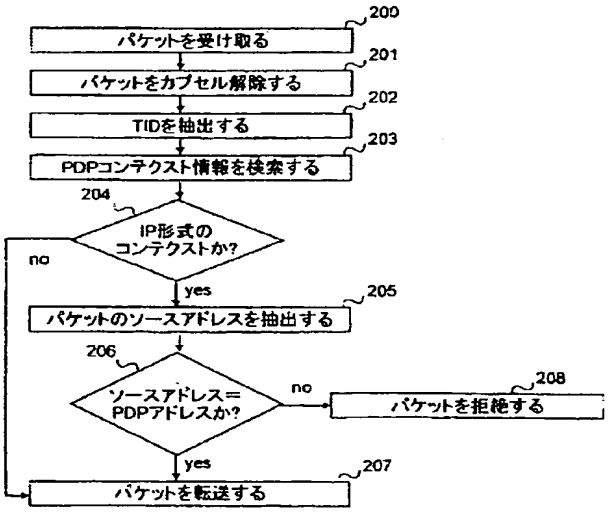
(21)出願番号　特願2001-547792(P2001-547792)
(86)(22)出願日　平成12年12月19日(2000.12.19)
(85)翻訳文提出日　平成14年6月20日(2002.6.20)
(86)国際出願番号　PCT/FI00/01114
(87)国際公開番号　WO01/047179
(87)国際公開日　平成13年6月28日(2001.6.28)
(31)優先権主張番号　19992767
(32)優先日　平成11年12月22日(1999.12.22)
(33)優先権主張国　フィンランド（ＦＩ）

(71)出願人　ノキア　コーポレイション
フィンランド　エフイーエン－02150　エスプー　ケイララーデンティエ　4
(72)発明者　ウスケラ　サミ
フィンランド　エフイーエン－00530　ヘルシンキ　シルタサーレンカトゥ　26　アー1
(72)発明者　ヨキネン　ハンヌ　テー
フィンランド　エフイーエン－03300　オタランピ　ヨキペロンティエ　375　アー
(74)代理人　弁理士　中村　稔　（外9名）

最終頁に続く

(54)【発明の名称】テレコミュニケーションシステムにおけるなりすましの防止

(57)【要約】
パケット無線ネットワークにおいて、ターミナルに対するパケットデータアドレスがアクチベートされて、ターミナルと外部ネットワークとの間にデータパケットを送信する。アクチベートされたパケットデータアドレスに関する情報は、少なくとも、ネットワークのエッジノードに記憶される。なりすまし即ち送信者データの偽った表示を防止するため、本発明の方法及びネットワークノードは、ターミナルから送信されたパケットのソースアドレスが、パケットの送信に使用されたパケットデータアドレスと同じであるかどうか、又はそのソースアドレスが許容パケットデータアドレスのリストに属するかどうかを上記ノードにおいてチェックする(206)ことを含む。上記両アドレスが同じであるか又はソースアドレスが許容パケットデータアドレスのリストに属する場合にのみ、パケットは、ノードから行先アドレスに向けて送信される(207)。



【特許請求の範囲】

【請求項１】　データパケットを送信することのできるターミナルと、第１サブシステム内でデータパケットを受信して転送するための少なくとも１つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法であって、上記第１サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第２サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第１サブシステムの少なくとも１つのノードにパケットデータアドレスを記憶し、そしてターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであるような方法において、

パケットのソースアドレスがパケットデータアドレスと同じであるかどうかを上記ノードにおいてチェックし(206)、そして

上記両アドレスが同じである場合にのみノードから行先アドレスに向けてパケットを送信する(207)、

という段階を備えたことを特徴とする方法。

【請求項２】　データパケットを送信することのできるターミナルと、第１サブシステム内でデータパケットを受信して転送するための少なくとも１つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法であって、上記第１サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第２サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第１サブシステムの少なくとも１つのノードにパケットデータアドレスを記憶し、そしてターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであるような方法において、

パケットデータアドレスを１組の許容パケットデータアドレスとして定義し、

パケットのソースアドレスが上記１組の許容パケットデータアドレスに属するかどうか上記ノードにおいてチェックし(206)、そして

パケットのソースアドレスが上記１組の許容パケットデータアドレスに属する場合にのみノードから行先アドレスに向けてパケットを送信する(207)、
という段階を備えたことを特徴とする方法。

【請求項３】　上記ノードは、ターミナルから第２サブシステムへデータパケットをルーティングする第１サブシステムのゲートウェイサポートノードである請求項１又は２に記載の方法。

【請求項４】　上記ノードは、移動ステーションにサービスするサポートノードであって、ターミナルから受け取ったパケットを第１サブシステムに向けてルーティングするサポートノードである請求項１又は２に記載の方法。

【請求項５】　上記第１サブシステムは、ＧＴＰプロトコルを使用するパケット無線ネットワークであり、そして上記パケットデータアドレスは、それに対応するＰＤＰコンテキストをアクチベートすることによりアクチベートされる請求項１ないし４のいずれかに記載の方法。

【請求項６】　上記方法は、更に、
第１パケットデータアドレスの形式に関する情報を上記ノードに維持し、この情報は、上記チェックが行われるところの少なくとも１つのパケットデータアドレス形式を含み、そして
パケットデータアドレスが第１パケットデータアドレス形式である場合にのみ上記チェックを実行する、
という段階を備えた請求項１ないし５のいずれかに記載の方法。

【請求項７】　上記第１パケットデータアドレス形式は、インターネットプロトコルに基づく少なくともＩＰアドレスを含む請求項６に記載の方法。

【請求項８】　パケットネットワークのターミナル(MS)から受信器(2,4)へデータパケットを送信するためのパケットネットワークのネットワークノード(SGSN,GGSN)であって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも１つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノード(SGSN,GGSN)において、

パケットを受信するのに応答して、パケットのソースアドレスを、ターミナルにより使用されるパケットデータアドレスと比較し、そして両アドレスが同一である場合にのみ、ネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成されたことを特徴とするネットワークノード(SGSN, GGSN)。

【請求項９】　パケットネットワークのターミナル(MS)から受信器(2, 4)へデータパケットを送信するためのパケットネットワークのネットワークノード(SGSN, GGSN)であって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも１つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノード(SGSN, GGSN)において、

上記パケットデータアドレスは、１組の許容パケットデータアドレスとして定義され、

パケットを受信するのに応答して、ネットワークノード(SGSN, GGSN)は、パケットのソースアドレスが、ターミナルにより使用されるパケットデータアドレスの上記１組の許容パケットデータアドレスに属するかどうかチェックし、そしてそのソースアドレスが上記１組の許容パケットデータアドレスに属する場合にのみネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成されたことを特徴とするネットワークノード(SGSN, GGSN)。

【請求項１０】　上記ネットワークノード(SGSN, GGSN)は、上記比較が実行されるところの第１パケットデータアドレス形式に関する情報を維持し、そしてターミナルにより使用されるパケットデータアドレスが第１パケットデータアドレス形式である場合にのみ比較を実行するよう構成された請求項８又は９に記載のネットワークノード。

【請求項１１】　上記ネットワークノードは、ＧＴＰプロトコルを使用するパケット無線ネットワーク(GPRS)のゲートウェイサポートノード(GGSN)である請求項８、９又は１０に記載のネットワークノード。

【請求項１２】　上記ネットワークノードは、ＧＴＰプロトコルを使用する

パケット無線ネットワーク(GPRS)においてターミナルにサービスするサポートノード(SGSN)である請求項８、９又は１０に記載のネットワークノード。

【発明の詳細な説明】

【０００１】

【技術分野】

本発明は、パケットデータを送信することのできるテレコミュニケーションシステムにおけるなりすましの防止に係る。より詳細には、本発明は、移動通信システムにおいて移動ステーションから送信されたＩＰ（インターネットプロトコル）パケットにおける送信者データのなりすましを防止することに係る。

【０００２】

【背景技術】

移動通信ネットワークは、移動データの送信用に実際のデータネットワークへのアクセスをユーザに与える有効なアクセスネットワークとして機能する。移動データ送信は、パン・ヨーロピアン移動通信システムＧＳＭ（移動通信用のグローバルシステム）のようなデジタル移動通信システムによって特に良好にサポートされる。本明細書において、「データ」という語は、デジタルテレコミュニケーションシステムにおいて送信されるいかなる情報も指す。このような情報は、デジタルエンコードされた音声及び／又は映像、コンピュータ間データトラフィック、テレファックスデータ、又はプログラムコードのショートセクション等を含む。移動通信システムとは、一般に、ユーザがシステムのサービスエリア内を移動するときにワイヤレス通信を使用するいかなるテレコミュニケーションシステムも指す。移動通信システムの典型的な例は、公衆地上移動ネットワークＰＬＭＮである。移動通信ネットワークは、外部ネットワーク、ホスト、又は特定のサービス手順により提供されるサービスへのワイヤレスアクセスをユーザに与えるアクセスネットワークであることがほとんどである。

【０００３】

移動通信システムを開発する主たる目標の１つは、移動ステーションがホストとしても機能し得るように移動通信ネットワークを経てＩＰサービスを利用する機会を提供することである。これは、例えば、汎用パケット無線サービスＧＰＲＳにおいて考えられる。ＧＰＲＳサービスは、ＧＳＭシステムにおいて移動データターミナルと外部データネットワークとの間にパケットデータ送信を与える。

ＧＰＲＳデータを送信及び受信するために、移動ステーションは、ＰＤＰ（パケットデータプロトコル）アクチベーション手順を要求することによりそれが使用を望むパケットデータアドレスをアクチベートしなければならない。このオペレーションは、移動ステーションを対応するゲートウェイサポートノードに知らしめ、従って、アクチベートされたパケットデータアドレスを使用して外部データネットワークとのインターワーキングを開始することができる。ＵＭＴＳ（ユニバーサル移動通信システム）及びＩＭＴ－２０００（国際移動テレコミュニケーション２０００）のような「第３世代移動通信システム」に対しても同様の解決策が構成されている。

【０００４】

特に、ＩＰネットワークでは、ＩＰデータパケットのソースアドレスのなりすまし即ち偽造が容易である。換言すれば、ＩＰパケットを送信するホストは、他の誰かであると偽り、そしてＡの名前でＢへパケットを送信し、Ｂは、Ａに応答を送信する。この場合に、Ａ及びＢの両方が互いに妨害する。この問題に対する１つの解決策は、ファイアウオールを使用することである。しかしながら、この解決策において、ユーザは認証されず、ソース及び行先アドレスのみが監視される。ファイアウオールでは、ソースアドレスが、通常、サブネットワークの精度で記述される。その結果、ファイアウオールは、パケットの真の送信者を知ることができず、同じサブネットワークのホストがそれら自体を互いに代表することができる。ファイアウオールに許されたソースアドレスを前もって知らねばならず、そして移動ステーションは、そのＩＰアドレスを変更せずに１つのファイアウオールのエリアから別のファイアウオールのエリアへ移動できねばならないので、ファイアウオールの許容ソースアドレスは、実際には、ファイアウオールによって保護されるサブネットワークにアクセスできる全ての移動ステーションをカバーする。これにより生じる問題は、ＩＰパケットのソースアドレスが信頼できるものでなく、なりすましを防止するために、移動ホストを別々に認証しなければならないことである。なりすましの防止は、ホストが課金されるＩＰサービスが利用されるときに特に重要である。しかしながら、信頼性の高い認証手順は、ネットワークの遅延を増加するか、或いは移動通信ネットワークの限定された

リソース即ちエアインターフェイスを浪費することになる。

【０００５】

【発明の開示】

本発明の目的は、データパケットの受信者が、データパケットのソースアドレスがパケットの真の送信者を示している事実を信頼できるようにする方法、及びこの方法を実施する装置を提供することである。

本発明のこの目的は、データパケットを送信することのできるターミナルと、第１サブシステム内でデータパケットを受信して転送するための少なくとも１つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法により達成される。この方法は、上記第１サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第２サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第１サブシステムの少なくとも１つのノードにパケットデータアドレスを記憶し、そしてターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであり、更に、パケットのソースアドレスがパケットデータアドレスと同じであるかどうかを上記ノードにおいてチェックし、そして両アドレスが同じである場合にのみノードから行先アドレスに向けてパケットを送信するという段階を備えている。

【０００６】

更に、本発明は、データパケットを送信することのできるターミナルと、第１サブシステム内でデータパケットを受信して転送するための少なくとも１つのノードとを備えたテレコミュニケーションシステムにおいてなりすましを防止するための方法であって、上記第１サブシステム内でターミナルに対するパケットデータアドレスをアクチベートしてターミナルと第２サブシステムとの間にデータパケットを送信し、パケットデータアドレスのデータパケットをルーティングする際に通る第１サブシステムの少なくとも１つのノードにパケットデータアドレスを記憶し、ターミナルから送信されたパケットを上記ノードで受け取り、パケットは、行先アドレス及びソースアドレスを含むものであり、更に、パケットデ

ータアドレスを１組の許容パケットデータアドレスとして定義し、パケットのソースアドレスが上記１組の許容パケットデータアドレスに属するかどうか上記ノードにおいてチェックし、そしてパケットのソースアドレスが上記１組の許容パケットデータアドレスに属する場合にのみノードから行先アドレスに向けてパケットを送信するという段階を備えた方法にも係る。

【０００７】

又、本発明は、パケットネットワークのターミナルから受信器へデータパケットを送信するためのパケットネットワークのネットワークノードであって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも１つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするよう構成されたネットワークノードにも係る。このネットワークノードは、パケットを受信するのに応答して、パケットのソースアドレスを、ターミナルにより使用されるパケットデータアドレスと比較し、そして両アドレスが同一である場合にのみ、ネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成されたことを特徴とする。

【０００８】

更に、本発明は、パケットネットワークのターミナルから受信器へデータパケットを送信するためのパケットネットワークのネットワークノードであって、ターミナルがデータパケットを送信するときに使用できるターミナルの少なくとも１つのパケットデータアドレスをアクチベートし、そしてターミナルから受け取ったパケットを、ターミナルにより使用されるパケットデータアドレスにアタッチするように構成されたネットワークノードにも係る。このネットワークノードは、パケットデータアドレスが１組の許容パケットデータアドレスとして定義され、パケットを受信するのに応答して、ネットワークノードが、パケットのソースアドレスが、ターミナルにより使用されるパケットデータアドレスの上記１組の許容パケットデータアドレスに属するかどうかチェックし、そしてそのソースアドレスが上記１組の許容パケットデータアドレスに属する場合にのみネットワークノードからパケットの行先アドレスに向けてパケットを送信するように構成

されたことを特徴とする。

【０００９】

本発明は、データパケットを送信するためにアクチベートされたパケットデータアドレスにより、例えば、ゲートウェイサポートノードＧＧＳＮは、データパケットを送信した移動ステーションのパケットデータアドレスを知るという考え方をベースとする。従って、ゲートウェイサポートノードＧＧＳＮは、データパケットのソースアドレスを、移動ステーションにより使用されるパケットデータアドレスと比較するだけでよい。両アドレスが同一である場合には、アドレスが偽造されたものではなく、パケットは、行先アドレスへ転送することができる。

本発明の効果は、実施が非常に簡単で、しかも、なりすましを防止できることである。例えば、ＩＰパケットの受信者は、ＩＰパケットのソースアドレスがＩＰパケットの送信者を認証するということを信頼することができる。付加的な認証メカニズムは必要とされず、従って、ネットワークに負荷がかからず、遅延を最小にすることができる。又、本発明は、課金可能なサービスの実施を容易にする。というのは、サービス創作者は、データパケットのソースアドレスが、課金されるべきユーザを指示することを信頼できるからである。

【００１０】

本発明の好ましい実施形態では、ゲートウェイサポートノードにおいて比較が行われる。この実施形態の効果は、ネットワーク内で数の少ない要素に比較メカニズムが追加されることである。

本発明の別の好ましい実施形態では、移動ステーションにサービスするパケット無線ネットワークのエッジノードにおいて比較が行われる。この実施形態の効果は、いずれにせよ供給されないパケットを送信することによりパケット無線ネットワークに負荷がかからないことである。

本発明の好ましい実施形態では、ソースアドレスのなりすまし即ち偽造を可能にするパケットデータプロトコルを使用するパケットに対してのみ比較が実行される。この実施形態の効果は、ソースアドレスを偽造できないパケットについては無益に比較が行われないことである。

本発明の方法及びネットワークノードの好ましい実施形態は、従属請求項に記

載する。

【００１１】

【発明を実施するための最良の形態】

以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。

本発明は、個々のパケットデータアドレスが、ＧＰＲＳシステムの場合ように、使用の前にアクチベートされ、そしてそのネットワークインフラストラクチャーにおいて情報がユーザのアクティブパケットデータアドレスに維持されるようないかなるパケット交換システムにも適用できる。これらのシステムは、「第３世代の移動通信システム」、例えば、ユニバーサル移動テレコミュニケーションシステム（ＵＭＴＳ）及びＩＭＴ－２０００（国際移動テレコミュニケーション）や、ＧＳＭシステムに対応する移動通信システム、例えば、ＤＣＳ１８００（１８８ＭＨｚ用のデジタルセルラーシステム及びＰＣＳ（パーソナル通信システム）や、上記システムをベースとしそしてＧＰＲＳ型のパケット無線を実施するＷＬＬシステムを含む。更に、本発明は、移動通信システム以外のシステム、例えば、ケーブルモデムネットワーク及び同様の固定システムにも適用することができる。本発明は、以下、ＧＳＭシステムのＧＰＲＳサービスを一例として使用して説明するが、このようなシステムに限定されるものではない。移動通信システムの定義は、急速に変化し、本発明に対して付加的な変更が必要となるであろう。このため、全ての用語及び表現は、広く解釈されるべきであり、そしてそれらは本発明を単に例示するものであって何らそれに限定されるものではないことを銘記されたい。

【００１２】

図１は、ＧＰＲＳサービスのネットワークアーキテクチャーを一般的なレベルで示す。というのは、ネットワークの詳細な構造は本発明に関与しないからである。ＧＳＭシステムの構造及び機能は、当業者にとって非常に馴染み深いものである。ＧＰＲＳサービスの構造は、例えば、参考としてここに取り上げるＥＴＳＩ仕様書０３．６０、バージョン６．０．０（デジタルセルラーテレコミュニケーションズシステム（フェーズ２＋）；汎用パケット無線サービス（ＧＰＲＳ）；サービス説明；段階２）に定義されている。ＧＰＲＳサービスは、無線アクセ

スを与えるアクセスネットワークを含み、これは、図１においてＧＳＭシステムのベースステーションサブシステムＢＳＳにより表わされる。又、ＧＰＲＳサービスは、パケットデータネットワークＰＤＮと移動ステーションＭＳとの間のデータのパケット交換送信に対してＧＰＲＳサービスのサポートノードをエッジノードとして備えている。サポートノードは、サービングＧＰＲＳサポートノードＳＧＳＮ及びゲートウェイＧＰＲＳサポートノードＧＧＳＮを含む。これらのサポートノードＳＧＳＮ及びＧＧＳＮは、バックボーンネットワーク１により相互接続される。ＳＧＳＮ及びＧＧＳＮの機能は、同じネットワークノードに物理的に結合することができ、この場合に、オペレータのバックボーンネットワークは不必要であることに注意されたい。しかしながら、論理的には、ノードは個別のノードである。

【００１３】

サービングＧＰＲＳサポートノードＳＧＳＮは、移動ステーションＭＳにサービスする。各サポートノードＳＧＳＮは、セルラーパケット無線ネットワークの１つ以上のセルのエリア内で移動データターミナル即ち移動ステーションＭＳに対してパケットデータサービスを生成する。このため、各サポートノードＳＧＳＮは、典型的に、ＧＳＭ移動通信システム（典型的にベースステーションサブシステムＢＳＳのベースステーションコントローラ）に接続され、中間の移動通信ネットワークがＳＧＳＮと移動ステーションとの間に無線アクセス及びパケット交換データ送信を与えるようにされる。換言すれば、セル内の移動ステーションＭＳは、無線インターフェイスを経てベースステーションと通信し、そして更にベースステーションサブシステムを経て、セルがサービスエリアに属するところのサポートノードＳＧＳＮと通信する。ＳＧＳＮノードの主たるファンクションは、そのサービスエリアにおいて新たなＧＰＲＳ移動ステーションを検出し、新たな移動ステーションＭＳのＧＰＲＳレジスタへの登録を実行し、データパケットをＧＰＲＳ移動ステーションへ送信し又はそこから受信し、そしてそのサービスエリア内の移動ステーションＭＳの位置についてファイルを維持することである。これは、ＳＧＳＮが、認証及び暗号化手順のようなセキュリティ機能及びアクセス制御を実行することを意味する。独特のトンネルを使用して、ＳＧＳＮは

、移動ステーションから受け取ったパケットをカプセル化形態でＧＰＲＳバックボーンネットワークを経てＧＧＳＮノードへルーティングし、そこで、パケットデータアドレスがアクチベートされる。

【００１４】

ＧＰＲＳゲートウェイサポートノードＧＧＳＮは、オペレータのＧＰＲＳネットワークを外部システム、データネットワーク、例えば、ＩＰネットワーク（インターネット）又はＸ．２５ネットワーク、及びサーバー２に接続する。又、ＧＧＳＮは、個人会社のネットワーク又はホストに直接接続することもできる。図１の例では、ＧＧＳＮは、信頼性のあるＩＰネットワーク３を経てサーバー２に接続され、そしてファイアウオールＦＷを経てインターネット４に接続される。ＧＧＳＮは、ＧＰＲＳ加入者のＰＤＰアドレス及びルーティング情報、即ちＳＧＳＮアドレスを含む。ＧＧＳＮは、移動ステーションＭＳのルートに関してＳＧＳＮノードによって発生されるルート情報を使用して位置ファイルを更新する。ＧＧＳＮは、外部アドレスと内部のルーティング情報（例えば、ＳＧＳＮ）との間のルーターとして機能する。換言すれば、ＧＧＳＮは、外部データネットワークのプロトコルパケットをカプセル化形態でＧＰＲＳバックボーンネットワークを経てＳＧＳＮノードへルーティングし、該ＳＧＳＮノードは、所与の時間に、移動ステーションＭＳにサービスする。又、これは、移動ステーションから送信されたパケットをカプセル解除し、そして外部データネットワークのパケットを関連データネットワークに送信する。又、ＧＧＳＮは、ある移動ステーションからネットワーク内の別の移動ステーションへパケットを送信する。更に、ＧＧＳＮは、データトラフィックの勘定についても役割を果たす。

【００１５】

移動ステーションＭＳは、パケットデータ送信をサポートしそしてネットワークへの無線インターフェイスを有するいかなる移動ノードでもよい。例えば、パケット無線オペレーションを行うことのできるセルラー電話に接続されたラップトップＰＣ、或いは小型コンピュータ及びパケット無線電話の一体化された組み合わせであってもよい。移動ステーションＭＳの他の実施形態は、種々のページャー、リモートコントローラ、監視及び／又はデータ収集装置、等を含む。又、

移動ステーションは、移動ノード又は移動ホストとも称される。

【００１６】

ＧＰＲＳサービスにアクセスするために、移動ステーションは、先ず、ＧＰＲＳアタッチオペレーションを実行することによりその存在をネットワークに知らしめねばならない。このオペレーションは、移動ステーションＭＳとＳＧＳＮノードとの間に論理的リンクを確立し、そして移動ステーションをＧＰＲＳを経てショートメッセージに使用できるようにするか、或いは同様のメッセージを接続なしに送信させ、ＳＧＳＮを経てページングを行いそして到来するＧＰＲＳデータを通知するようにさせる。より正確さを期すために、移動ステーションＭＳがＧＰＲＳネットワークにアタッチするときに（ＧＰＲＳアタッチ手順において）、ＳＧＳＮは、移動管理コンテクスト（MMコンテクスト）を形成し、そしてプロトコル層において移動ステーションＭＳとＳＧＳＮノードとの間に論理リンクＬＬＣ（論理リンク制御）が確立される。MMコンテクストは、ＳＧＳＮノード及び移動ステーションＭＳに記憶される。ＳＧＳＮノードのMMコンテクストは、加入者のＩＭＳＩ、ＴＬＬＩ（一時的論理リンク識別子）、位置及びルーティング情報等の加入者データを含む。

【００１７】

ＧＰＲＳデータを送信及び受信するために、移動ステーションＭＳは、ＰＤＰアクチベーション手順を要求することにより、ＰＤＰアドレス、即ちそれが使用を望むパケットデータアドレスをアクチベートしなければならない。ＰＤＰコンテクストは、移動ステーションがＧＰＲＳネットワークにアタッチするときにアクチベートすることができる。或いは又、移動ステーションは、ＰＤＰコンテクストを後でアクチベートしてもよいし、又はＧＰＲＳネットワークから受け取られたアクチベーション要求の結果としてアクチベーションが実行されてもよい（ＧＰＲＳネットワーク要求ＰＤＰコンテクストアクチベーション）。ＧＰＲＳインターフェイスは、パケットデータアドレス及びそれに関連したパラメータを記述する１つ以上の個々のＰＤＰコンテクストを含む。より詳細には、ＰＤＰコンテクストは、ＰＤＰ形式（例えば、Ｘ．２５又はＩＰ）、ＰＤＰアドレス（例えば、ＩＰアドレス）、サービスクオリティＱｏＳ及びＮＳＡＰＩ（ネットワーク

サービスアクセスポイント識別子）のような種々のデータ送信パラメータを定義する。１つの移動ステーションは、多数の同様のＰＤＰアドレス、例えば、異なるＩＰアドレスをＰＤＰアドレスとしてもつことができる（即ち、移動ステーションは、多数のＩＰ型コンテクストを有する）。例えば、ＩＰプロトコルを使用して送信される種々のクオリティ及び価格のサービスに対して種々のＩＰアドレス即ちコンテクストを使用することができる。ＰＤＰコンテクストのパケットデータアドレスは、永久的（即ちホーム位置レジスタの加入者データにおいて定義される）であるか、又は動的であり、この場合は、ＧＧＳＮがＰＤＰアクチベーション手順の間にパケットデータアドレスを割り当てる。ＰＤＰアクチベーション手順は、ＰＤＰコンテクストをアクチベートし、そして移動ステーションを対応するＧＧＳＮノードに知らしめ、その結果、外部データネットワークとのインターワーキングを開始させる。ＰＤＰコンテクストアクチベーションの間に、ＰＤＰコンテクストが移動ステーション並びにＧＧＳＮ及びＳＧＳＮノードに生成される。ＰＤＰコンテクストがアクチベートされると、ユーザがＧＳＭ手順により認証され、従って、ＰＤＰコンテクストアクチベーションにおいてターミナルに与えられるパケットデータアドレス、例えば、ＩＰアドレスを、ユーザの認識コード、例えば、ＩＭＳＩ（国際移動加入者認識）に確実にアタッチすることができる。

【００１８】

ＰＤＰコンテクストが生成され、そしてＧＴＰプロトコル（ＧＰＲＳトンネリングプロトコル）を用いてパケットがトンネル送信される。移動ステーションＭＳは、ＰＤＰコンテクストを特定のメッセージ「アクチベートＰＤＰコンテクスト要求」でアクチベートし、この場合、移動ステーションは、ＴＬＬＩ、ＰＤＰ形式、要求されたＱｏＳ及びＮＳＡＰＩに関する情報、及び任意であるがＰＤＰアドレス及びアクセスポイント名ＡＰＮに関する情報を与える。ＳＧＳＮは、「クリエートＰＤＰコンテクスト」メッセージをＧＧＳＮノードに送信し、該ノードは、ＰＤＰコンテクストを生成して、それをＳＧＳＮノードに送信する。「アクチベートＰＤＰコンテクスト要求」メッセージ（及び「クリエートＰＤＰコンテクスト」メッセージ）がＰＤＰアドレスを含まない場合には、ＧＧＳＮは、Ｐ

ＤＰコンテクストの生成中にＰＤＰアドレスを割り当て、そしてＳＧＳＮへ送信されるべきＰＤＰコンテクストに動的なＰＤＰアドレスを含む。ＳＧＳＮは、ＰＤＰコンテクストを「アクチベートＰＤＰコンテクスト応答」メッセージにおいて移動ステーションＭＳへ送信する。ＰＤＰコンテクストは、移動ステーションＭＳ、ＳＧＳＮノード及びＧＧＳＮノードに記憶される。サービングＳＧＳＮノードでは、各ＰＤＰコンテクストがMMコンテクストと共に記憶される。ＭＳが新たなＳＧＳＮノードのエリアへローミングするときには、新たなＳＧＳＮが古いＳＧＳＮノードからMMコンテクスト及びＰＤＰコンテクストを要求する。

【００１９】

従って、ＰＤＰコンテクストアクチベーション手順では、移動ステーションＭＳとＧＧＳＮノードとの間に仮想接続又はリンクが確立される。同時に、このＰＤＰコンテクスト及びパケットデータアドレスに対してＧＧＳＮとＳＧＳＮとの間に独特のトンネルが形成される。トンネルは、ＩＰパケットがたどるルートであり、これにより、移動ステーションから送信されたパケットは、ＧＧＳＮにおいてあるＰＤＰコンテクスト及びあるパケットデータアドレスにアタッチされる。換言すれば、トンネルは、パケットを送信するときに使用される移動ステーションのパケットデータアドレスを識別するのに使用される。パケットは、ＴＩＤ（トンネル識別子）と共に、又はＧＴＰプロトコルが使用されるときにはトンネルエンドポイント識別子と共に、あるＰＤＰコンテクストにアタッチされる。ＴＩＤは、ＮＳＡＰＩ及びＩＭＳＩを含む。ＰＤＰコンテクストアクチベーション手順の間に、ＧＧＳＮは、ＰＤＰコンテクストを指すのに使用されるべきトンネルエンドポイント識別子を割り当ててもよい。

【００２０】

図２は、ゲートウェイサポートノードＧＧＳＮにおいて本発明の第１の好ましい実施形態によるオペレーションを示すフローチャートである。本発明の第１の好ましい実施形態では、パケットに含まれたソースアドレスが、その形式がなりすましを可能にするＰＤＰコンテクストのみにおいて、アクチベートされたパケットデータアドレスと比較される。これらは、ＩＰ形式のコンテクスト及びパケットデータアドレスを含む。これらの形式（又は１つの形式）は、比較を実行す

るノードにおいて定義される。図２の例では、なりすましが、ＩＰアドレスについてのみ可能であり、他のパケットデータアドレス形式では成功しないと仮定する。又、移動ステーションは、それが使用するＰＤＰコンテクスト（即ち、例えばＩＰアドレスを仮定する）をアクチベートし、そしてＩＰパケットを、例えば図１に示すサーバー１又はインターネット４に送信すると仮定する。更に、トンネルを識別するのにＴＩＤが使用されると仮定する。

【００２１】

図２を参照すれば、ステップ２００において、ＧＧＳＮは、独特のトンネルを使用してパケットを受信し、ステップ２０１においてそれをカプセル解除し、そしてステップ２０２においてトンネル識別子ＴＩＤを抽出する。ステップ２０３において、ＧＧＳＮは、ＴＩＤにより、ＴＩＤに対応するＰＤＰコンテクストのＰＤＰコンテクスト情報を検索する。この情報は、パケットデータアドレス、この例ではＩＰアドレスで表わされたＰＤＰアドレスを含む。次いで、ステップ２０４において、ＧＧＳＮは、トンネルに対応するＰＤＰコンテクスト（即ちパケットデータアドレス）がＩＰ形式のものであるかどうかチェックする。もしそうであれば、ＧＧＳＮは、ステップ２０５において、パケットのタイトルに与えられたソースアドレスを抽出する。ＧＧＳＮは、両方のアドレスを知ると、それらをステップ２０６において比較する。ソースアドレスが、ＰＤＰコンテクストのＰＤＰアドレスと同じである場合には、移動ステーションは、ＩＰパケットに含まれることを請求し、その結果、ＧＧＳＮは、ステップ２０７においてパケットを転送する。ソースアドレスがＰＤＰアドレスと相違する場合には、移動ステーションは、別の移動ステーションを偽称し、それ故、ＧＧＳＮは、ステップ２０８においてパケットを拒絶する。ここで、拒絶とは、パケットが行先アドレスに送信されないことを意味する。

【００２２】

拒絶の後にパケットに何が起きるかは、オペレータの定義に依存し、本発明には関わりない。例えば、ユーザ及びターミナルは、制御平面シグナリングを使用することにより、ソースアドレスが然るべきものでないことが通知されてもよい。例えば、ＧＧＳＮは、アラームメッセージをオペレータのネットワークオペレ

ーション及びメンテナンスセンターに送信してもよい。又、ＰＤＰコンテクスト情報及びパケット情報を含むエントリーをエラーログファイルへ行うこともできる。又、拒絶されたパケットの内容がエラーログファイルに書き込まれてもよい。更に、ユーザ及びターミナルに偽のソースアドレスであることを通知する更に別の形態は、不正パケットを送信するのに使用されたＰＤＰコンテクストをデアクチベートすることである。ＰＤＰコンテクストは、例えば、ＧＧＳＮ、ＳＧＳＮ及びＭＳにおいてデアクチベートされ、従って、ＧＧＳＮは、ＰＤＰコンテクストをデアクチベートするようにＳＧＳＮに要求し（又はパケットを拒絶するのがＳＧＳＮである場合にはＳＧＳＮがデアクチベーション要求をＧＧＳＮに送信し）、そしてＳＧＳＮは、ＰＤＰコンテクストをデアクチベートするようにＭＳに要求する。デアクチベーション要求メッセージは、ＭＳ又はＭＳに関連したアプリケーションが偽の又は不正なソースアドレスを使用したことを指示する特定のデアクチベーションコードを原因コードとして含むのが好ましい。この特定の原因コードの結果として、ユーザには、偽のソースアドレスを使用する試みであることが通知される。この通知を使用する主たる理由は、ユーザが不正行為を思いとどまるようにするか、又はユーザに偽のソースアドレスを使用したアプリケーションが通知されることである。エンドユーザへの通知は、偽のソースアドレスでデータを送信しようと試みたアプリケーションを識別するテキストメッセージ又はメッセージウインドウであるのが好ましい。又、上述した動作は、所定量の不正パケットが拒絶された後にのみ実行されてもよい。偽のソースアドレスの使用がＭＳに通知されると、例えば、ＧＧＳＮがＭＳ及び／又はオペレータネットワーク及びメンテナンスセンターに送信するメッセージは、偽のソースアドレスを有するパケットの上位層プロトコル（例えば、ＴＣＰ又はＵＤＰ）ヘッダに関するある情報を搬送するのが好ましい。これは、不正のアプリケーション及び不正活動の目的を容易に見出せるようにする。メッセージは、拒絶されたパケットの全内容を含んでもよい。拒絶されたパケットのパケット流は、オペレータのネットワークオペレーション及びメンテナンスセンターのような外部ノードへ転送されてもよい。

【００２３】

ステップ２０４において、ＰＤＰがＩＰ形式でないことが通知された場合に、ＧＧＳＮは、ステップ２０７へ直接進み、そしてパケットを転送する。

ステップ２０６におけるチェックの目的は、誰か別の者を偽っていない送信者のパケットだけがＧＧＳＮにより外部ネットワークに転送されるように確保することである。本発明により送信者を認証するには簡単なチェックだけで充分であり、認証シグナリングは必要とされない。

【００２４】

本発明の別の好ましい実施形態では、ステップ２０６のチェックがＳＧＳＮにおいて実行され、そしてステップ２０１が省略される。というのは、移動ステーションから受信されるパケットがカプセル化されないからである。他の好ましい実施形態では、ＳＧＳＮが、ステップ２０２において、ＴＩＤではなく、ＭＳから受信したパケットからＴＬＬＩ及びＮＳＡＰＩを抽出する。ＴＬＬＩは、ルーティングエリア内でＭＳ、ひいては、ＩＭＳＩを独特に識別する。ＮＳＡＰＩは、このパケットと共にＭＳにより使用されるＰＤＰコンテクストを識別する。ＴＬＬＩ及びＮＳＡＰＩを使用して、ＳＧＳＮは、ＰＤＰコンテクスト情報を検索する。他の好ましい実施形態では、ＴＩＤ（又はＰＤＰコンテクストを識別する他の対応する情報）がパケットに追加され、そしてパケットは、ステップ２０７の前に、即ちパケットがＧＧＳＮに送信される前に、カプセル化される。

【００２５】

将来、ＰＤＰアドレスのアドレススペースは、１つのＰＤＰコンテクストに関連されるか、或いは対応する接続定義に関連されることになろう。アドレススペースは、例えば、許容ＰＤＰアドレスのリストである。この場合に、パケットに含まれるソースアドレスは、この許容アドレス間にあれば充分である。同様に、将来、許容ＰＤＰアドレスの一部分を定義することにより、ＰＤＰコンテクスト情報は、許容ＰＤＰアドレスを１組の許容アドレス（即ちアドレススペース）として指定することができる。この場合に、パケットのソースアドレスは、アドレスの定義された部分を含まねばならず、即ちソースアドレスは、１組の許容アドレスに属していなければならない。又、アドレススペースは、上述の両方の方法を使用することにより定義されてもよい。アドレススペースは、他の何らかの方

法で定義することもできる。

【００２６】

なりすましを可能にする多数のパケットデータアドレス形式が定義される実施形態では、ステップ２０４において、パケットに使用されるパケットデータアドレスがそれらの１つであるかどうかチェックされる。もしそうであれば、ステップ２０５から続ける。さもなければ、ステップ２０７へ進む。

本発明のある好ましい実施形態では、パケットに含まれたソースアドレスは、アクチベートされたパケットデータアドレスの形式には関わりなく、アクチベートされたパケットデータアドレスと比較される。この場合に、ステップ２０４のチェックは行われず、ステップ２０６のチェックが各パケットに対して実行される。

【００２７】

図２に示すステップの順序は、上述したものとは異なってもよく、又、それらステップは、同時に実行することもできる。例えば、ステップ２０４は、ステップ２０１の前に実行することができ、そしてステップ２０３は、ステップ２０５と同時に実行することができる。それらのステップ間に、図示されていないステップを実行することもできる。ある実施形態では、ステップ２０１及び／又は２０４を省略することもできる。ステップ２０２では、ＴＩＤに代わって、ＰＤＰコンテクストを識別する他の情報を抽出することができる。

【００２８】

現状技術によるサービスを実施するのに必要な手段に加えて、本発明の機能を実施するテレコミュニケーションシステム、テレコミュニケーションネットワーク及びネットワークノードは、パケットに含まれたアドレスを、パケットの送信者に対してアクチベートされた即ち許容されたアドレス（１つ又は複数）と比較するための手段を備えている。既存のネットワークノードは、本発明による機能に使用できるプロセッサ及びメモリを備えている。本発明を実施するのに必要な全ての変更は、付加的な又は更新されたソフトウェアルーチンとして及び／又はアプリケーション回路（ＡＳＩＣ）により実施することができる。

ネットワークのエッジ要素（ＳＧＳＮ又はＧＧＳＮ）が加入者を認証すること

を上記で説明したが、本発明は、エッジ要素に限定されるものではない。比較に必要なアドレス情報が記憶される別のネットワークノードが比較を実行することもできる。

【００２９】

上記の「パケットデータプロトコルＰＤＰ」又は「ＰＤＰコンテクスト」という語は、一般に、ターミナル（例えば移動ステーション）の状態及び少なくとも１つのネットワーク要素又は機能を指すものと理解されたい。この状態は、ターミナルにより使用されるネットワーク（例えば移動通信ネットワーク）を経て、データパケットに対する特定数のパラメータを有する送信経路、即ちトンネルを生じさせる。又、ここで使用する「ノード」という語は、ＰＤＰトンネルを経て送信されるデータパケットを処理するネットワーク要素又は機能を一般的に指す用語であると解釈されたい。

上記説明及び添付図面は、本発明を単に例示するものに過ぎないことを理解されたい。特許請求の範囲に規定された本発明の精神及び範囲から逸脱せずに種々の変更がなされ得ることが当業者に明らかであろう。

【図面の簡単な説明】

【図１】

ＧＰＲＳサービスのネットワークアーキテクチャーを示すブロック図である。

【図２】

本発明による動作を示すフローチャートである。

【図１】

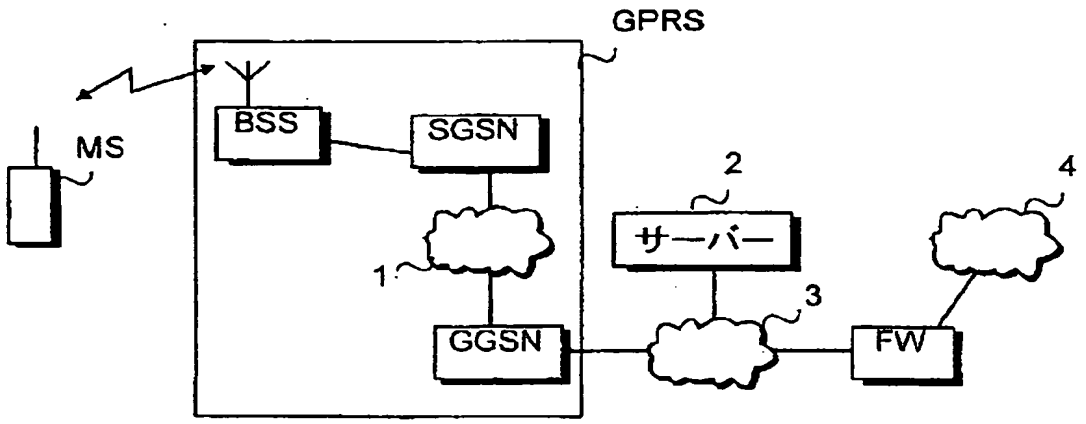


FIG.1

【図２】

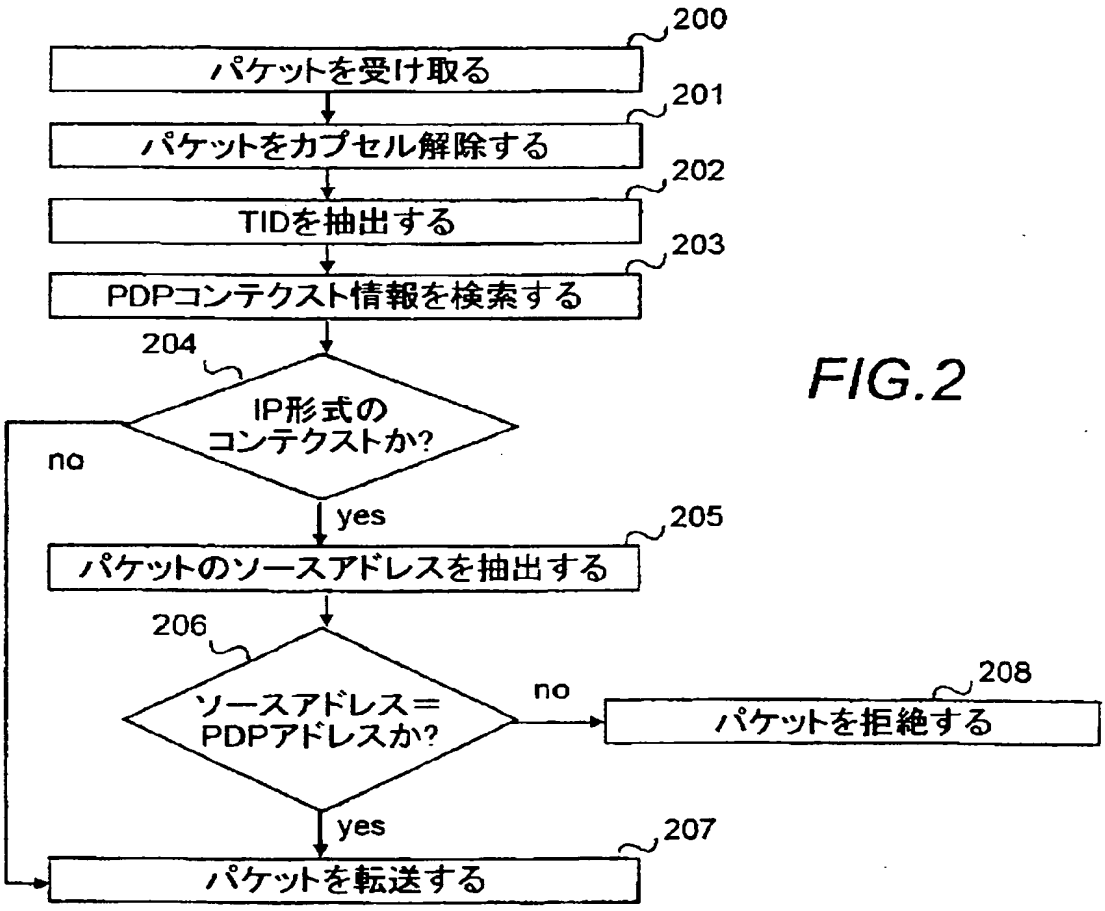


FIG.2

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/01114

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32, H04L 12/00, H04L 12/28
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9948303 A2 (CISCO TECHNOLOGY, INC.), 23 Sept 1999 (23.09.99), page 4, line 26 - page 7, line 20, figures 2,3, claims 1-14, abstract --	1-12
Y	WO 9917499 A2 (NOKIA TELECOMMUNICATIONS OY), 8 April 1999 (08.04.99), page 8, line 6 - line 29, figure 3, claims 1-20, abstract --	1-12

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 2001	30 -03- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Klas Arvidsson/JAn Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/01114

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	1997 IEEE Symposium on Proceedings, Security and Privacy. "Analysis of a denial of service attack on TCP" Schuba, C.L., et al Page 210, column 2, line 25 - page 211, column 1, line 52; page 214, column 2, line 19 - page 217, column 2, line 9. Figures 8,9,11 -- --------	1-12

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/FI 00/01114

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9948303 A2	23/09/99	AU 3098299 A	11/10/99
WO 9917499 A2	08/04/99	AU 9351598 A	23/04/99
		CN 1277771 T	20/12/00
		EP 1018241 A	12/07/00
		FI 973806 A	27/03/99

Form PCT/ISA/210 (patent family annex) (July 1998)

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

Fターム(参考) 5K030 GA15 HA08 HC01 HC09 HD03 KA05 LB05 LC15
5K067 AA30 BB21 DD17 GG01 GG11 HH05 HH22 HH24